NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 8705.2B
Effective Date: May 06, 2008
Expiration Date: May 06, 2013

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Human-Rating Requirements for Space Systems (w/change 1 dated 12/7/2009)

Responsible Office: Office of Safety and Mission Assurance

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixF | AppendixE | ALL |

Chapter 3 Technical Requirements for Human-Rating

3.1 Overview

3.1.1 The technical requirements in this chapter identify capabilities in three primary categories:

a. System Safety

b. Crew/Human Control of the System

c. Crew Survival/Aborts

3.1.2 As stated previously in this NPR, these requirements are not intended to be all inclusive or an absolute prescription for human-rating. Compliance with these requirements does not assure a safe system for human missions into space. These technical requirements are intended to provide the foundation of capabilities upon which the Program Manager will build by identifying and incorporating additional unique capabilities for each reference mission (see paragraph 2.3.2). Furthermore, some of these requirements were intentionally written to force the design team to bound the problem. The design team should evaluate the intent of these technical requirements and use their talents to deliver the safest practical system that will accomplish the mission within the constraints. Technical requirements, along with history's lessons, legacy solutions, expert opinions, and best practices, are only as good as the implementer's understanding of their origins and assumptions.

3.1.3 The technical requirements are presented in sections to clearly identify the applicable mission phase and applicable system type. The term "space system" (defined in Appendix A) includes the crewed space system and all space-based and ground-based systems that functionally interact with the crewed space system during the mission.

3.2 System Safety Requirements

3.2.1 The space system shall provide the capability to sustain a safe, habitable environment for the crew (Requirement 58503).

Rationale: Protection from the hazardous environment of space or the hazardous environment at the planetary surface is fundamental to crew survival. Also, the space system should be inherently safe or designed to minimize risk (e.g., no exposed sharp edges, no exposed high temperature surfaces). This requirement includes protection from known environments such as space radiation hazards and lunar dust. Providing a habitable environment is also fundamental to the integration of the human into the space system. In order for the crew to contribute to the safe conduct of the mission, their basic habitability needs to be met.

3.2.2 The space system shall provide failure tolerance to catastrophic events (minimum of one failure tolerant), with the specific level of failure tolerance (one, two or more) and implementation (similar or dissimilar redundancy) derived from an integrated design and safety analysis (per the requirement in paragraph 2.3.7.1) (Requirement). Failure of primary structure, structural failure of pressure vessel walls, and failure of pressurized lines are excepted from the failure tolerance requirement provided the potentially catastrophic failures are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance. Other potentially catastrophic hazards that cannot be controlled using failure tolerance are excepted from the failure tolerance requirements with concurrence from the Technical Authorities provided the hazards are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance.

Rationale: The overall objective is to provide the safest design that can accomplish the mission given the constraints imposed on the program. Since space system development will always have mass, volume, schedule, and cost constraints, choosing where and how to apply failure tolerance requires integrated analyses at the system level to assess safety and mission risks. First and foremost, the failure tolerance is applied at the overall system level - to include all capabilities of the system. While failure tolerance is a term frequently used to describe minimum acceptable redundancy, it may also be used to describe two similar systems, dissimilar systems, cross-strapping, or functional interrelationships that ensure minimally acceptable system performance despite failures, or additional features that completely mitigate the effects of failures. Even when assessing failure tolerance at the integrated system level, the increased complexity and the additional utilization of system resources (e.g. mass, power) required by a failure tolerant design may negatively impact overall system safety as the level of failure tolerance is increased.

Ultimately, the level and type of redundancy (similar or dissimilar) is an important and often controversial aspect of system design. Since redundancy does not, by itself, make a system safe, it is the responsibility of

the engineering and safety teams to determine the safest practical system design given the mission requirements and constraints. Additionally, the overall system reliability is a significant element of the integrated safety and design analysis used in the determination of the level of redundancy. Redundancy alone without sufficient reliability does not meet the intent of this requirement.
When a critical system fails because of improper or unexpected performance due to unanticipated conditions, similar redundancy can be ineffective at preventing the complete loss of the system. Dissimilar redundancy is very effective provided there is sufficient separation among the redundant legs. (For example, dissimilar redundancy where the power for all redundant capability was routed through a common conduit would not survive a failure where the conduit was severed). It is also highly desirable that the spaceflight system performance degrades in a predictable fashion to allow sufficient time for failure detection and, when possible, system recovery even when experiencing multiple failures.

There are examples of dissimilar redundancy in current systems. For Earth reentry, the Soyuz spacecraft has a dissimilar backup ballistic entry mode to protect for loss of the primary attitude control system and a backup parachute for landing. Other examples include backup batteries for critical systems that protect for loss of the primary electrical system and the use of pressure suits during reentry to protect for loss of cabin pressure.

Ultimately, the program and Technical Authorities evaluate and agree on the failure scenarios/modes and determine the appropriate level of failure tolerance and the practicality of using dissimilar redundancy or backup systems to protect for common cause failures.

Where failure tolerance is not the appropriate approach to control hazards, specific measures need to be employed to: (1) Recognize the importance of the hazards being controlled; (2) Ensure robustness of the design; and (3) Ensure adequate attention/focus is being applied to the design, manufacture, test, analysis, and inspection of the items. In the area of design, in addition to the application of specifically approved standards and specifications, these measures can include identification of specific design features which minimize the probability of occurrence of failure modes, such as application of stringent factors of safety or other design margins. For manufacture, these measures can include establishing special process controls and documentation, special handling, and highlighting the importance of the item for those involved in the manufacturing process. For test, this can include accelerated life testing, fleet leader testing program, testing to understand failure modes or other testing to establish additional confidence and margin in the design. For analysis (in lieu of tests), these measures can include correlation with testing representative of the actual configuration and the collection, management, and analysis of data used in trending failures, verifying loss of crew requirements, and evaluating flight anomalies. For inspection, these measures can include identification of specific inspection criteria to be applied to the item or the application of Government Mandatory Inspection Points for important characteristics of the item. This approach to hazard control takes advantage of existing standards or standards approved by the Technical Authorities to control

hazards associated with the physical properties of the hardware and are typically controlled via application of margin to the environments experienced by the design or system properties effected by the environment. Acceptance of these approaches by the Technical Authorities avoids processing waivers for numerous hazard causes where failure tolerance is not the appropriate approach. This includes, but is not limited to, Electro-Magnetic Interference, Ionizing Radiation, Micrometeoroid Orbital Debris, structural failure, pressure vessel failure, and aerothermal shell shape for flight.

3.2.3 The space system shall provide the failure tolerance capability in 3.2.2 without the use of emergency equipment and systems (Requirement 58557).

Rationale: Emergency systems and equipment, such as fire suppression systems, fire extinguishers and emergency breathing masks, launch/entry pressure suits, and systems used exclusively for launch aborts, should not be considered part of the failure tolerance capability since these emergency systems and equipment cannot definitely prevent a catastrophic initiating event. In the example of the fire extinguisher, the fire can burn out of control and overwhelm the capability of the extinguisher. Emergency systems are there to mitigate the effects of a hazard, when the first line of defense, in the form of failure tolerance, cannot prevent the occurrence of the hazardous situation. Catastrophic events, as defined in this NPR and consistent with NPR 8715.3, NASA General Safety Program Requirements, include crew fatality and the unplanned loss/destruction of a major element of the crewed space system during the mission that could potentially lead to death or permanent disability of the crew or passengers. Aborts, when used to prevent a catastrophic event, may be considered part of the failure tolerance of the system. However, when aborts are used to remove the crew from the catastrophic event (e.g., abort on Earth ascent in the presence of a launch vehicle explosion), the catastrophic event has not been prevented and the abort system (even though it may save the crew and passengers) cannot be considered as a leg of failure tolerance to the catastrophic event.

3.2.4 The space system shall be designed to tolerate inadvertent operator action (minimum of one inadvertent action), as identified by the human error analysis (paragraph 2.3.11), without causing a catastrophic event (Requirement 58559).

Rationale: An operator is defined as any human that commands or interfaces with the space system during the mission, including humans in the control centers. The appropriate level of protection (i.e., one, two or more inadvertent actions) is determined by the integrated human error and hazard analysis described in 2.3.11.

3.2.5 The space system shall tolerate inadvertent operator action, as described in 3.2.4, in the presence of any single system failure (Requirement 58561).

Rationale: The intent of this requirement is to provide a robust human-system interface design that cannot be defeated by a system failure. Where the system is designed to protect for more than one inadvertent action, the level of protection after a single system failure may be reduced - but still protects from a single inadvertent operator action.

3.2.6 The space system shall provide the capability to mitigate the hazardous behavior of critical software where the hazardous behavior would result in a catastrophic event (Requirement 58563).

Rationale: According to current software standards, the software system will be designed, developed, and tested to: 1) Prevent hazardous software behavior. 2) Reduce the likelihood of hazardous software behavior. 3) Mitigate the negative effects of hazardous software behavior. However, for complex software systems, it is very difficult to definitively prove the absence of hazardous behavior. Therefore, the crewed system has the capability to mitigate this hazardous behavior if it occurs. The mitigation strategy will depend on the phase of flight and the "time to effect" of the potential hazard. Hazardous behavior includes erroneous software outputs or performance.

3.2.7 The space system shall provide the capability to detect and annunciate faults that affect critical systems, subsystems, and/or crew health (Requirement 58569).

Rationale: A fault is defined as an undesired system state. A failure is an actual malfunction of a hardware or software item's intended function. The definition of the term "fault" envelopes the word "failure," since faults include other undesired events such as software anomalies and operational anomalies. It is necessary to alert the crew to faults (not just failures) that affect critical functions.

3.2.8 The space system shall provide the capability to isolate and/or recover from faults identified during system development that would result in a catastrophic event (Requiremer (Requirement 58572).

Rationale: This capability is not intended to imply a failure tolerance capability or expand upon the failure tolerance capability. The intent is to provide isolation and recovery from faults where the system design (e.g., redundant strings or system isolation) enables the implementation of this capability. Also, any faults identified during system development should be protected by isolation and/or recovery. However, it is acknowledged that not all faults that would cause catastrophic events can be detected or isolated in time to avoid the event. Similarly, system design cannot ensure that once the fault is detected and isolated that a recovery is always possible. However, in these cases, isolation of the fault should prevent the catastrophic event.

3.2.9 The space system shall provide the capability to utilize health and status data (including system performance data) of critical systems and subsystems to facilitate anomaly resolution during and after the mission (Requirement 58574).

Rationale: Access to health and status data is a key element of anomaly resolution during the mission, which could prevent the crew from executing an abort or prevent the situation from developing into a catastrophic event. Resolving anomalies between missions is just as important. This requirement intentionally does not specify a crash survivable data recorder. That determination is left for the program. The program also determines what data should be available to facilitate anomaly resolution.

3.2.10 The crewed space system shall provide the capability for autonomous operation of system and subsystem functions which, if lost, would result in a catastrophic event (Requirement 58576).

Rationale: This capability means that the crewed system does not depend on communication with Earth (e.g., mission control) to perform functions that are required to keep the crew alive.

3.2.11 The space system shall provide the capability for the crew to readily access equipment involved in the response to emergency situations and the capability to gain access to equipment needed for follow-up/recovery operations (Requirement 58578).

Rationale: Fire extinguishers are one example of the type of equipment needed for immediate response to a fire emergency. "Ready access" means that the crew is able to access the equipment in the time required without the use of tools. The ready access time will depend on the phase of flight and the time to effect of the hazard. Ready access also accounts for suited crew members if the equipment could be needed during a mission phase or operation where the crew is suited. A contamination clean-up kit is an example of equipment needed for follow up/recovery operations.

3.3 System Control Requirements - General

3.3.1 The crewed space system shall provide the capability for the crew to monitor, operate, and control the crewed space system and subsystems, where:

a. The capability is necessary to execute the mission; or

b. The capability would prevent a catastrophic event; or

c. The capability would prevent an abort (Requirement).

Rationale: This capability flows directly from the definition of human-rating. Within the context of this requirement, monitoring is the ability to determine where the vehicle is, its condition, and what it is doing. Monitoring helps to create situational awareness that improves the performance of the human operator and enhances the mission. Determining the level of operation over individual functions is a decision made separately for specific space systems. Specifically, if a valve or relay can be controlled by a computer, then that same control could be offered to the crew to perform that function. However, a crewmember probably could not operate individual valves that meter the flow of propellant to the engines, but the function could be replaced by a throttle that incorporates multiple valve movements to achieve a desired end state (reduce or increase thrust). Meeting any of the three stated conditions invokes the requirement. The first condition recognizes that the crew performs functions to meet mission objectives and, in those cases, the crew is provided the designated capabilities. This does not mean that the crew is provided these capabilities for all elements of a mission. Many considerations are involved in making these determinations, including capability to perform the function and reaction time. The second and third conditions recognize that, in many scenarios, the crew improves the performance of the system and that the designated capabilities support that performance improvement.

3.3.2 The crewed space system shall provide the capability for the crew to manually override higher level software control/automation (such as automated abort initiation, configuration change, and mode change) when the transition to manual control of the system will not cause a catastrophic event (Requirement 58586).

Rationale: This is a specific capability necessary for the crew to control the crewed space system. While this capability should be derived by the program per paragraph 3.3.1, the critical nature of software control and automation at the highest system level dictates specific mention in the NPR. Therefore, the crew has the capability to control automated configuration changes and mode changes, including automated aborts, at the system level as long as the transition to manual control is feasible and will not cause a catastrophic event. The program and Technical Authorities will determine the appropriate implementation of this requirement - which is documented in the HRCP.

3.3.3 The space system shall provide the capability for humans to remotely monitor,

operate, and control the crewed system elements and subsystems, where:

a. The remote capability is necessary to execute the mission; or

b. The remote capability would prevent a catastrophic event; or

c. The remote capability would prevent an abort (Requirement 58598).

Rationale: This capability will likely be implemented using a mission control on Earth. Logically, there will be times when the crew is unavailable to monitor, operate, and control the system. If the crew vacates one element of the system or transfers to another Human-Rated system as part of the reference mission, there is a capability for humans to monitor the unoccupied elements. In some of these cases, the crew may be able to perform this function from their new location. In other cases, mission control may perform this function.

This capability is not intended to force 100 percent of communication coverage for all elements of the system. The communication coverage is planned to implement the capability to meet the three conditions.

For EVA suits, this capability does not mean that the EVA suit requires constant monitoring between EVAs (missions). If the suit is powered off and stowed, periodic checks or inspections may be all that is required.

3.4 System Control Requirements - Human-Rated Spacecraft

3.4.1 The crewed space system shall provide the capability for the crew to manually control the flight path and attitude of their spacecraft, with the following exception: during the atmospheric portion of Earth ascent when structural and thermal margins have been determined to negate the benefits of manual control (Requirement).

Rationale: The capability for the crew to control the spacecraft's flight path is a fundamental element of crew survival. Manual control means that the crew can bypass the automated guidance of the vehicle to interface directly with the flight control system to effect any flight path within the capability of the flight control system. Limiting the crew to choices presented by the automated guidance function is not a valid implementation of manual control. Manual control does not mean the capability to bypass the flight control system. Also, for phases of flight where there is no active control of the spacecraft, such as when under passive parachutes, then manual control cannot be provided and this requirement would not apply. For a space station, when there is no propulsion system available for reboost, then manual control of the flight path (orbital parameters) cannot be provided, and this requirement would not apply. During the atmospheric portion of Earth ascent (approximately the first 100,000 feet), where the trajectory and attitude are tightly constrained to maintain positive structural and thermal margins, the trajectory and attitude constraints are not typically available independent of guidance. In this case, if the only option is for the crew to follow guidance then nothing is gained by manual control over automated control.

3.4.2 The crewed spacecraft shall exhibit Level 1 handling qualities (Handling Qualities Rating (HQR) 1, 2 and 3), as defined by the Cooper-Harper Rating Scale, during manual control of the spacecraft's flight path and attitude (Requirement).

Rationale: Level 1 handing qualities are the accepted standard for manual control of flight path and attitude in military aircraft. Level 1 handling qualities will allow the crew to

effectively control the spacecraft when necessary for mission completion or to prevent a catastrophic event. Reference NASA TND-5153 for the Cooper-Harper Rating Scale.

3.5 System Control Requirements - Proximity Operations with Human-Rated Spacecraft

3.5.1 The space system shall provide the capability for the crew to monitor, operate, and control an uncrewed spacecraft during proximity operations, where:

a. The capability is necessary to execute the mission; or

b. The capability would prevent a catastrophic event; or

c. The capability would prevent an abort (Requirement 58604).

Rationale: Proximity operations cover several scenarios, but this term is specifically defined as two (or more) systems operating in space (not on a planetary surface) within the prescribed safe zone for either system. When an uncrewed space system is the active spacecraft performing proximity operations with a crewed spacecraft, this requirement includes the capability for the crew to monitor the trajectory of the uncrewed system. At a minimum, the crewed system will have the capability to send basic trajectory commands to hold/stop, continue, and breakout to the uncrewed spacecraft. Active means the spacecraft is changing the flight path/trajectory/orbital parameters to effect the desired result during proximity operations.

3.5.2 The crewed space system shall provide the capability for direct voice communication between crewed spacecraft (2 or more) during proximity operations (Requi (Requirement 58607).

Rationale: Direct voice communication means that the signal is not routed through mission control on Earth or another communication relay satellite.

3.6 Crew Survival/Abort Requirements

3.6.1 Earth Ascent Systems

3.6.1.1 The space system shall provide the capability for unassisted crew emergency egress to a safe haven during Earth prelaunch activities (Requirement 58611).

3.6.1.2 The space system shall provide abort capability from the launch pad until Earth-orbit insertion to protect for the following ascent failure scenarios (minimum list):

a. Complete loss of ascent thrust/propulsion (Requirement 58613).

b. Loss of attitude or flight path control (Requirement 58614).

Rationale: Flying a spacecraft through the Earth's atmosphere to orbit entails inherent risk. Three crewed launch vehicles have suffered catastrophic failures during ascent or on the launch pad (one Space Shuttle and two Soyuz spacecraft). Both Soyuz crews survived the catastrophic failure due to a robust ascent abort system. Analysis, studies, and past experience all provide data supporting ascent abort as the best option for the crew to survive a catastrophic failure of the launch vehicle. Although not specifically stated, the ascent abort capability incorporates some type of vehicle monitoring to detect failures and, in some cases, impending failures.

3.6.1.3 The crewed space system shall monitor the Earth ascent launch vehicle performance and automatically initiate an abort when an impending catastrophic failure is detected (Requirement 58616).

Rationale: Launch vehicle performance monitoring may include specific system or subsystem performance. The program will determine the appropriate parameters to monitor in the launch vehicle. Not all potentially catastrophic failures can be detected prior to manifestation. Similarly, system design and analysis cannot guarantee the crew will survive all catastrophic failures of the launch system, but the abort system should provide the best possible chance for the crew to survive. When an impending catastrophic failure of the launch vehicle is detected, the time to effect requires the abort system to be initiated automatically. Also, if the catastrophic failure itself is detected by a monitoring system, the abort is initiated automatically. This is not intended to require independent implementation by the crewed space system of capabilities inherent to the launch vehicle (the launch vehicle is part of the crewed space system).

3.6.1.4 Earth Ascent Abort

3.6.1.4.1 The space system shall provide the capability for the crew to initiate the Earth ascent abort sequence (Requirement 58619).

3.6.1.4.2 The space system shall provide the capability for the ground control to initiate the Earth ascent abort sequence (Requirement 58620).

Rationale: The crew and ground control will likely have access to more data than an automated abort system. Therefore, both the crew and ground control have the capability to initiate the abort when necessary for crew survival.

3.6.1.5 If a range safety destruct system is incorporated into the design, the space system shall automatically initiate the Earth ascent abort sequence when range safety destruct commands are received onboard, with an adequate time delay prior to destruction of the launch vehicle to allow a successful abort (Requirement 58622).

Rationale: Prior to destruction of the launch vehicle by means of a range safety destruct (flight termination) system, the abort system is initiated. An automated initiation of the abort sequence provides the best chance for crew survival while protecting the public from a range safety violation. It is left to the program to determine which range safety command (arm or fire) will result in the initiation of the abort sequence.

3.6.2 Earth Orbit Systems

3.6.2.1 The crewed space system shall provide the capability to autonomously abort the mission from Earth orbit by targeting and performing a deorbit to a safe landing on Earth (R (Requirement 58625).

3.6.3 Earth - Lunar Transit and Lunar Orbit Systems

3.6.3.1 The crewed space system shall provide the capability to autonomously abort the mission during lunar transit and from lunar orbit by executing a safe return to Earth (Requir (Requirement 58627).

3.6.4 Lunar Descent Systems

3.6.4.1 The crewed space system shall provide the capability to autonomously abort the lunar descent and execute all operations required for a safe return to Earth (Requirement 58629).

Rationale: The extent of abort coverage is to be determined by the program. The goal is 100 percent coverage during the descent.

3.6.5 Lunar Surface Systems

3.6.5.1 The space system shall provide the capability for the crew on the lunar surface to monitor the descent and landing trajectory of an uncrewed spacecraft and send commands necessary to prevent a catastrophic event (Requirement 58632).

Rationale: This capability assumes the arrival is within the safe zone of the crew or crewed surface systems.

3.6.6 Lunar Ascent Systems

Reserved for a future version of the NPR.

3.6.7 Earth Reentry Systems

3.6.7.1 The crewed space system shall provide the capability for unassisted crew emergency egress after Earth landing (Requirement 58636).

Rationale: This requirement assumes the crew is able to function in a 1-g environment. Unassisted means without help from ground or rescue personnel or equipment.

3.6.7.2 The crewed space system shall provide a safe haven capability for the crew inside the spacecraft after Earth landing until the arrival of the landing recovery team or rescue forces(Requirement 58638).

Rationale: If the crew is physically unable to egress the spacecraft or does not choose to egress the spacecraft due to a hazardous environment outside, then the spacecraft provides a safe haven until the arrival of recovery forces. This requirement is not intended to establish the boundaries of the hazardous environment (for example, the maximum sea state) or the duration of the safe haven. The program, with concurrence from the Technical Authorities, specifies these conditions in their requirements documents. The nominal return to Earth will have well established timelines and expectations for the habitation conditions inside the spacecraft. Conversely, after an ascent abort or emergency return to Earth, the timeline may be less certain and the expectations of comfort will be different from the nominal mission return.

3.6.7.3 The space system shall provide recovery forces with the location of the spacecraft after return to Earth (Requirement 58640).

Rationale: In the event of a contingency, the spacecraft may not return to the nominal preplanned location. Experience has shown that the system needs to provide a means for recovery forces to be provided with the spacecraft location. The ISS Expedition 6 crew returned to Earth in a Soyuz spacecraft. A system failure caused the Soyuz to downmode to a ballistic entry. When this happened, the Soyuz landed 'short' of the targeted landing zone. The system could not provide the recovery forces with an accurate location and the crew was placed in a survival situation while waiting for recovery. Subsequently, the Soyuz system was modified with a location system for recovery forces. This system was successfully utilized on Expedition 15, when another ballistic entry occurred.

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixF | AppendixE | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS